

**Notice of Allowability**

Application No.

10/790,045

Applicant(s)

SANO ET AL.

Examiner

Art Unit

Salvatore Cangialosi

3621

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 9/29/05.
2. ☒ The allowed claim(s) is/are 14-17.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some\* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date \_\_\_\_\_
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

*Salvatore Cangialosi*  
**SALVATORE CANGIALOSI**  
**PRIMARY EXAMINER**  
**ART UNIT 222**

**The following is an Examiner's Statement of Reasons for Allowance**

Regarding independent claim 1, the prior art fails to show a computer-readable storage medium storing a program for controlling an encryption/decryption unit for encrypting a plaintext into a cipher text and/or decrypting into a plaintext, the program including: first encryption/decryption means for performing an encryption or decryption process, first substitution means for performing data substitution of an output from said first encryption/decryption means according to a predetermined permutation table, second encryption/decryption means for performing an encryption or decryption process for an output from said first substitution means; second substitution means for performing data substitution of an output from said second encryption/decryption means according to a predetermined permutation table; third encryption/decryption means for performing an encryption or decryption process for an output from said second substitution means; key generating means for generating intermediate keys respectively supplied to said first, second, and third encryption/decryption means and said first and second substitution means; and said first and second substitution means functioning to perform identity conversion when the intermediate key generated by said key generating means contains predetermined data; said key generating means comprises: dividing means for dividing key data K of a predetermined number of bits

Serial Number: 10/790,045  
Art Unit: 3621

3

into a plurality of data and storing the divided data into respective registers, expanded permutation means for reading out the divided key data from the respective registers and effecting an expanded permutation on the divided key data; DES-SS key schedule means for generating intermediate keys K1 and K3 from a result of the expanded permutation performed by said expanded permutation means, DES key schedule means for generating an intermediate key K2 from a result of the expanded permutation performed by said expanded permutation means, and substitution schedule means for generating intermediate keys KKI and KK2 from the contents of the registers in the manner and complexity recited by the claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the Issue Fee and to avoid processing delays should preferably accompany the Issue Fee. Such submissions should be clearly labeled Comments on Statement of Reasons for Allowance.

Any inquiry concerning this communication should be directed to Salvatore Cangialosi at telephone number (703) 305-1837. The examiner can normally be reached 6:30 Am to 5:00 PM, Tuesday through Friday. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell, can be reached at (703) 305-9768.

**Any response to this action should be mailed to:**

Serial Number: 10/790,045  
Art Unit: 3621

4

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450


or faxed to (703)872-9306

Hand delivered responses should be brought to

United States Patent and Trademark Office  
Customer Service Window  
Randolph Building  
401 Dulany Street  
Alexandria, VA 22314

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Technology Center 3600 Customer Service Office whose telephone number is (703) 306-5771.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
SALVATORE CANGIALOSI  
PRIMARY EXAMINER  
ART UNIT 222